Polityka Bezpieczeństwa Powiatowy Urząd Pracy w Gryfinie

Zasady i procedury użytkowników systemów informatycznych w Powiatowym Urzędzie Pracy w Gryfinie

Spis treści

Wprowadzenie

Dokument opisuje procedury bezpieczeństwa danych osobowych zawartych w systemach informatycznych PUP Gryfino. Opisane zbiory zasad i procedur określają granice dopuszczalnego zachowania wszystkich użytkowników systemu informatycznego wspomagającego pracę urzędu. Dokument zawiera również opis konsekwencji, jakie mogą ponieść osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Podstawowymi wymaganiami stawianymi współczesnym systemom informatycznym są odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania.

Politykę bezpieczeństwa należy rozumieć jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji o danych osobowych wewnątrz organizacji. Jest obowiązującym dokumentem określającym procedury zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji w PUP Gryfino.

Celem utworzenia instrukcji jest podniesienie bezpieczeństwa dokumentów i systemów informatycznych, w których są gromadzone i przetwarzane dane oraz określenie odpowiedzialności pracowników za prawidłowe działanie tych systemów i bezpieczeństwo przetwarzanych w nim danych. Polityka bezpieczeństwa wprowadza również procedury dotyczące stwierdzenia naruszenia zabezpieczenia systemu informatycznego oraz postępowań w wypadku klęski żywiołowej.

Za przestrzeganie zasad ochrony i bezpieczeństwa danych w komórkach organizacyjnych odpowiedzialni są kierownicy tych komórek. Administrator Danych jest zobowiązany do przeprowadzania okresowych kontroli mających na celu potwierdzenie prawidłowego przestrzegania zasad ochrony bezpieczeństwa danych w komórkach organizacyjnych. Rolę Administratora Danych w urzędzie pełni Dyrektor PUP Gryfino.

Podstawa prawna:

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 nr 100 poz. 1024)
- Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. 2005 nr 171 poz. 1433)
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: DZ. U. 2002r. Nr 101 poz. 926 ze zmianami)
- Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz. U. 2003 nr 3 poz. 25 z późn. Zm.)
- Art. 47 i 51 Konstytucji Rzeczpospolitej Polskiej

Definicje

Według Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 1997 r. Nr 133 poz. 883) z rozdziału 1 artykułu 3:

1) Ustawę stosuje się do organów państwowych oraz samorządu terytorialnego, a także do innych państwowych i komunalnych jednostek organizacyjnych oraz podmiotów niepaństwowych realizujących zadania publiczne.
2) Ustawę stosuje się również do osób fizycznych i prawnych oraz jednostek organizacyjnych niemających osobowości prawnej, które przetwarzają dane w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych.
3) Ustawę stosuje się do podmiotów określonych w ust. 1 i 2, które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, nie mają siedziby albo miejsca zamieszkania na terytorium Rzeczypospolitej Polskiej, a przetwarzają dane przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej.
4) Ustawy nie stosuje się do osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych.

Według Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 1997 r. Nr 133 poz. 883) z rozdziału 1 artykułu 6:[1]

1) W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
2) Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
3) Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Według Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101 poz. 926) z rozdziału 1 artykułu 7 (z uwzględnionymi poprawkami ustawy z dnia 22

[1] W brzmieniu ustalonym przez art. 1 pkt 1 ustawy z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych (Dz.U. Nr 100, poz. 1087), która weszła w życie z dniem 3 października 2001 r.

stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujące kierownicze stanowiska państwowe), ilekroć w ustawie jest mowa o:

1) zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2) przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
3) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,[2]
4) zabezpieczeniu danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5) usuwaniu danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6) Administratorze Danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ust. 1 i 2, decydujące o celach i środkach przetwarzania danych osobowych,
7) zgodzie osoby, której dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,
8) odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
   a) osoby, której dane dotyczą,
   b) osoby upoważnionej do przetwarzania danych,
   c) przedstawiciela, o którym mowa w art. 31a,
   d) podmiotu, o którym mowa w art. 31,
   e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem

[2] Dodany przez art. 1 pkt 2 ustawy, o której mowa w przypisie 1.

9) państwie trzecim – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego.

Według Rozporządzenia Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego z rozdziału 1 §2 ilekroć w rozporządzeniu jest mowa o:

1) incydencie bezpieczeństwa teleinformatycznego – należy przez to rozumieć każde zdarzenie naruszające bezpieczeństwo teleinformatyczne spowodowane w szczególności awarią systemu lub sieci teleinformatycznej, działaniem osób uprawnionych lub nieuprawnionych do pracy w tym systemie lub sieci albo zaniechaniem osób uprawnionych;
2) przekazywaniu informacji niejawnych – należy przez to rozumieć zarówno transmisję informacji niejawnych, jak i przekazywanie elektronicznego nośnika danych, na którym zostały one utrwalone;
3) przetwarzaniu informacji niejawnych – należy przez to rozumieć także wytwarzanie, przechowywanie lub przekazywanie informacji niejawnych.

Według Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Ilekroć w rozporządzeniu jest mowa o:

1) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych zwaną dalej ustawą;
2) identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym;
3) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
4) sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73. poz. 852, z późn. zm.);

5) sieci publicznej – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne;
6) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
7) rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
8) integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
9) raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
10) poufność danych rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
11) uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Dodatkowe definicje

1) Administrator Systemów Informatycznych (ASI) – osoba zajmująca się siecią informatyczną w jednostce.
2) Odbicie dysków (ang. Disk mirroring) jest procesem tworzenia wielokrotnych kopii lustrzanych na wielu dyskach, zapewniając tym samym, że mechaniczne uszkodzenie dysku lub jego odłączenie nie spowoduje utraty danych;
3) systemy zamienne (ang. Failover systems) są to dwa lub więcej systemów monitorujących wzajemną poprawność działania, w przypadku awarii, system sprawny przejmuje kontrolę nad zasobami;
4) autoryzacja - weryfikacja uprawnień w systemie np. dostęp do określonych funkcji, czy też danych;
5) dokument elektroniczny - zbiór danych wprowadzanych lub przechowywanych na dowolnym nośniku przez system informatyczny lub podobny układ, które mogą być odczytane lub wyświetlone przez osobę lub przez tego rodzaju system lub układ, a także wszelkiego rodzaju prezentacja i wszelkiego rodzaju przedstawienie tych danych w formie drukowanej lub innej. (akt prawny Unii Europejskiej: w decyzji Komisji 2004/563/WE2[3])

[3] Decyzja Komisji z 7 lipca 2004 r. zmieniająca jej regulamin wewnętrzny (2004/563/WE, Euratom)

Informacje wstępne

1) Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:
   - stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   - stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji sieci informatycznej mogą wskazywać lub sugerować naruszenie zabezpieczeń tych danych.
2) Polityka bezpieczeństwa obowiązuje wszystkich pracowników oraz stażystów PUP Gryfino.
3) Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych.
4) Administrator Danych, którym jest Dyrektor wyznacza Administratora Bezpieczeństwa Informacji dla danych zawartych w systemach informatycznych Urzędu oraz osobę upoważnioną do zastępowania Administratora Bezpieczeństwa Informacji.
5) Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:
   - ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych,
   - podejmowania stosownych działań zgodnie z niniejszą Polityką Bezpieczeństwa w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
   - niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   - nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.
6) Osoba zastępująca Administratora Bezpieczeństwa Informacji powyższe zadania realizuje tylko w przypadku nieobecności Administratora Bezpieczeństwa Informacji.
7) Osoba zastępująca składa Administratorowi Bezpieczeństwa Informacji relację z podejmowanych działań w czasie jego zastępstwa.

ROZDZIAŁ I

Opis zdarzeń naruszających ochronę danych osobowych.

1. Podział zagrożeń:
   a) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
   b) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
   c) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na:
      - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
      - nieuprawniony dostęp do systemu z jego wnętrza,
      - nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania,
      - bezpośrednie zagrożenie materialnych składników systemu.

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe
   a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   b) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie silnego pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
   c) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym fakt pozostawienia serwisantów bez nadzoru,

d) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
e) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenie systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
f) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
g) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
h) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
i) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń np. login użytkownika i jego hasło,
j) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
k) ujawniono istnienie nieautoryzowanych kont dostępu do danych,
l) podmieniono, lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w inny sposób niedozwolony skasowano lub skopiowano dane osobowe,
m) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowano się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony uważa się również stwierdzone nieprawidłowości w zakresie bezpieczeństwa miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, nośnikach cyfrowych itp.

Rozdział II

Zabezpieczenie danych osobowych

1. Administratorem Danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu jest Dyrektor PUP Gryfino.

2. Administrator Danych osobowych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych PUP Gryfino, a w szczególności:

   a) zabezpieczyć dane przed udostępnienie ich osobom nieupoważnionym,
   b) zapobiegać przed zabraniem/kradzieżą danych przez osoby nieuprawnioną,
   c) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Do zastosowanych środków technicznych należy:

   a) zabezpieczenie wejścia do pomieszczeń, w których przetwarzane są dane osobowe,
   b) szczególne zabezpieczenie centrum przetwarzania danych (serwer i serwerownia),
   c) zabezpieczenie stacji roboczych użytkowników komputerów programowe (antywirus, firewall) oraz systemowe (hasło dostępu),
   d) zabezpieczeniu stacji roboczej przy odejściu od biurka poprzez „zablokowanie komputera"
   e) wyposażenie pomieszczeń w szafy z zamkami patentowymi umożliwiające zabezpieczenie dokumentacji.

4. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:

   a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,

b) przeszkolenie osób, o których mowa w pkt. a, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochrona danych osobowych,

c) kontrolowanie otwierania i zamykania pomieszczeń, w którym są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę z pracy.

d) wprowadzenie wyraźnego zakazu pozostawiania samych petentów w pomieszczeniach PDO.

5. Niezależnie od zasad opisanych w niniejszym dokumencie w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

ROZDZIAŁ III

Kontrola przestrzegania zasad zabezpieczania danych osobowych

1. Administrator Danych wyznacza spośród pracowników PUP Gryfino, Administratora Bezpieczeństwa Informacji (ABI), który sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie. Jednocześnie Administrator Danych wskazuje osobę pełniącą zastępstwo Administratora Bezpieczeństwa Informacji (ABI).

1.1. Zakres obowiązków Administratora Bezpieczeństwa Informacji (ABI)

a) Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane oraz kontrolą przebywających w nich osób. Pomieszczenia te powinny być zabezpieczone przed dostępem do nich osób nie posiadających uprawnień do przetwarzania danych. Osoby takie mogą przebywać w nich jedynie w obecności osób uprawnionych. Na czas nieobecności zatrudnionych tam osób, pomieszczenia te powinny być odpowiednio zabezpieczone.
b) Czuwa nad wdrażaniem „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" oraz dba o bieżące jej uaktualnienie, stosownie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych Urzędu.
c) Określa strategię zabezpieczenia systemów informatycznych Urzędu.
d) Zapewnia awaryjne zasilanie komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania. Komputery oraz urządzenia, o których mowa wyżej, powinny być zasilane poprzez zastosowanie specjalnych urządzeń podtrzymujących zasilanie. Urządzenia te powinny być wyposażone w oprogramowania umożliwiające bezpieczne wyłączenie systemu komputerowego. Oznacza to takie wyłączenie, w którym przed zanikiem zasilania zostaną prawidłowo zapisane rozpoczęte transakcje na bazie danych oraz wszelkie inne działanie w ramach pracujących aplikacji i oprogramowania systemowego.

e) Nadzór, aby komputery przenośne, w których przetwarzane są dane, zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby komputery te nie były udostępniane osobom nieupoważnionym do przetwarzania danych. Osoby posiadające komputery przenośne lub inne urządzenia jak palmtopy, pen drive, flash disck lub tzw. dyski wymienne z zapisanymi w nich danymi, należy przeszkolić. Szkolenie dotyczy zachowania szczególnej uwagi podczas transportu, przechowywania oraz odpowiedniego zabezpieczenia urządzeń w pomieszczeniu.

f) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane. Dyski i inne informatyczne nośniki danych zawierające dane przeznaczone do likwidacji, należy pozbawić zapisu tych danych, a w przypadku, gdy nie jest to możliwe należy uszkodzić w sposób uniemożliwiający ich odczyt. Urządzenia przekazywane do naprawy należy pozbawić zapisanych danych lub naprawiać w obecności osoby upoważnionej przez Administratora Bezpieczeństwa Informacji.

g) Nadzór czynności związanych z zabezpieczeniem pod kątem obecności wirusów komputerowych, częstotliwości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji.

h) Nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu.

i) Nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych.

j) Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.

k) Nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane generowane przez system informatyczny. W zakresie nadzoru, o którym mowa wyżej, Administrator Bezpieczeństwa Informacji powinien dopilnować, aby osoby zatrudnione przy przetwarzaniu danych miały dostęp do niszczarki dokumentów w celu niszczenia błędnie utworzonych lub niepotrzebnych już wydruków komputerowych z danymi.

l) Nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych a w szczególności:

- ustalenie identyfikatorów użytkowników i ich haseł (identyfikatory użytkowników należy wpisać do ewidencji osób zatrudnionych przy przetwarzaniu danych).
- dopilnowanie, aby hasła użytkowników były zmieniane co najmniej raz na miesiąc,
- dopilnowanie, aby dostęp do danych przetwarzanych w systemie był możliwy wyłączenie po podaniu identyfikatora i właściwego hasła,
- dopilnowanie, aby hasła użytkowników były trzymane w tajemnicy (również po upływie terminu ich ważności),
- dopilnowanie, aby identyfikatory osób, które utraciły uprawnienia do przetwarzania danych osobowych zostały natychmiast wyrejestrowane, a hasła unieważnione.

m) Identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Urzędu.

n) Określa potrzeby w zakresie zabezpieczania systemów informatycznych, w których przetwarzane są dane.

o) Może wyznaczyć osobę pełniącą funkcję Administratora Sieci oraz ją nadzorować

p) Nadzoruje działania zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych.

q) Zgłasza potrzeby w zakresie zmian w konfiguracji sprzętu lub oprogramowania mających wpływ na bezpieczeństwo systemu komputerowego.

r) Nadzór, aby ekrany monitorów stanowisk komputerowych, na których przetwarzane są dane, automatycznie się wyłączyły po upływie ustalonego czasu nieaktywności użytkownika i stosowanie takich wygaszaczy ekranowych, które po upływie określonego czasu bezczynności użytkownika wygaszają monitor i jednocześnie uruchamiają blokadę, która uniemożliwia kontynuowanie pracy na komputerze bez podania właściwego hasła. Wygaszacz taki oprócz ochrony danych, które przez dłuższy okres czasu wyświetlane byłyby na ekranie monitora, chroni system przed przechwyceniem sesji dostępu do danych przez nieuprawnioną osobę. W pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

s) Podejmuje natychmiastowe działania zabezpieczające stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych.

t) Analizuje sytuacje, okoliczności i przyczyny, które doprowadziły do naruszenia bezpieczeństwa danych i przygotowuje oraz przedstawia przełożonemu odpowiednie zmiany do „Instrukcji zarządzania systemem informatycznym". Zmiany te powinny być takie, aby wyeliminować lub ograniczyć wystąpienie podobnych sytuacji w przyszłości. Obowiązek śledzenia skuteczności zabezpieczeń, o którym mowa wyżej, oraz obowiązek ich udoskonalania, nałożony na Administratora Bezpieczeństwa Informacji, wynika bezpośrednio z obowiązku podejmowania odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

1.2. Zadania ABI;

a) ABI realizuje zadania w zakresie ochrony danych, a w szczególności:

- ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych PUP Gryfino.
- podejmowanie stosownych działań zgodnie z „Polityką Bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych, znajdujących się w systemie informatycznym,
- niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
- nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

W przypadku nieobecności ABI powyższe zadania realizuje osoba zastępująca ABI. **Osoba zastępująca składa ABI pisemną relację z podejmowanych działań w czasie jego zastępstwa.**

b) ABI opracowuje plan roczny w zakresie realizacji Polityki Bezpieczeństwa, który zawiera:

- zakres, sposób i czas zapoznania się pracowników z Polityką Bezpieczeństwa,
- terminarz szkoleń z zakresu wprowadzanych procedur,
- terminarz szkoleń stanowiskowych,
- terminarz wprowadzania do stosowania poszczególnych elementów Polityki Bezpieczeństwa,

- termin kontroli stosowania wszystkich postanowień wprowadzonych Polityką Bezpieczeństwa,
- sprawdzenie funkcjonowania procedur poprzez symulację jednego z zagrożeń określonych w Instrukcji postępowania w sytuacji naruszania systemu ochrony danych osobowych,
- analizę zgodności innych wewnętrznych aktów prawa z Polityką Bezpieczeństwa a w przypadku stwierdzonych niezgodności - harmonogram dostosowania ich postanowień do wymogów Polityki Bezpieczeństwa,
- zestawienie zawierające potrzeby w zakresie dostosowania struktury organizacyjnej oraz stosowanego sprzętu i oprogramowania.

c) ABI sporządza roczne plany kontroli zatwierdzane przez Dyrektora i zgodnie z nimi przeprowadza kontrole oraz dokonuje oceny stanu bezpieczeństwa danych osobowych.

d) Na podstawie zgromadzonych materiałów, o których mowa w ust. 2, ABI sporządza roczne sprawozdanie i przedstawia Administratorowi Danych.

ROZDZIAŁ IV

Postępowanie w przypadku naruszenia ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia:

   a) zabezpieczenia systemu informatycznego,
   b) technicznego, fizycznego stanu urządzeń,
   c) zawartości zbioru danych osobowych,
   d) ujawnienia metody pracy lub sposobu działania programu,
   e) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   f) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar itp.)

   osoba zatrudniona przy przetwarzaniu danych osobowych jest zobowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.

2. W razie niemożności zawiadomienia Administratora Bezpieczeństwa Informacji, lub osoby zastępującej Administratora, należy powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa Informacji lub osoby go zastępującej, należy:

   a) niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn i sprawców,
   b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   c) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,

d) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
e) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
f) zastosować się do innych instrukcji i regulaminów, jeśli odnoszą się one do zaistniałego przypadku,
g) udokumentować wstępnie zaistniałe naruszenie (Załącznik nr 12),
h) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby go zastępującej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba go zastępująca:

a) rozpoznaje zaistniałą sytuację i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
b) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
c) rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu Administratora danych,
d) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami.

5. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który niezwłocznie przekazuje Administratorowi danych, a w przypadku jego nieobecności osobie uprawnionej. Raport powinien zawierać w szczególności:

a) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
b) określenie czasu i miejsca naruszenie i powiadomienia,
c) określenie okoliczności towarzyszących i rodzaju naruszenia,
d) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
e) wstępną ocenę przyczyn wystąpienia naruszenia,

f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa Informacji zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo PUP Gryfino i Administratora Bezpieczeństwa Informacji.

9. Analiza o której mowa w ust. 8, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

ROZDZIAŁ V

Postanowienia końcowe

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

2. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych do niniejszego dokumentu.

3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa Informacji.

4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002r. Nr 101, poz. 926) oraz możliwość wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

5. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002r. Nr 101, poz. 926), rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100,

poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

6. Niniejsza „Polityka Bezpieczeństwa" wchodzi w życie z dniem jej podpisania.

Spis załączników:

Załącznik 1. Zarządzenie Dyrektora dotyczące powołania ABI

Załącznik 2. Zarządzenie dyrektora dotyczące powołania Z-cy ABI

Załącznik 3. Upoważnienie do Przetwarzania Danych Osobowych

Załącznik 4. Upoważnienie do przebywania w pomieszczeniach PDO

Załącznik 5. Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa

Załącznik 6. Wykaz budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane

Załącznik 7. Wykaz zbiorów przetwarzanych elektronicznie lub w inny sposób

Załącznik 8. Wniosek o przeszkolenie przez ABI

Załącznik 9. Wniosek o zarejestrowanie użytkownika

Załącznik 10. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Załącznik 11. Wzór raportu z naruszenia zasad bezpieczeństwa systemu informatycznego

Załącznik 12. Opis struktur zbiorów danych wskazujący zawartości poszczególnych pól informacyjnych i powiązania między nimi.

Załącznik nr 1

Zarządzenie Dyrektora PUP
...

ZARZĄDZENIE NR ...
z dnia ...
Dyrektora Powiatowego Urzędu Pracy w Gryfinie

w sprawie powołania **„Administratora Bezpieczeństwa Informacji"** i **„Administratora Systemów Informatycznych"** w Powiatowym Urzędzie Pracy w Gryfinie i jego Filii w Chojnie.

Na podstawie:

- § 17 pkt 16 Regulaminu Organizacyjnego Powiatowego Urzędu Pracy w Gryfinie w związku z:
- art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity DzU z 2002 roku Nr 101, poz. 926 z późn. zm.),
- art.71 – 76 ustawy z dnia 29 września 1994 roku o rachunkowości (tekst jednolity Dz.U. z 2009r Nr 152, poz. 1223 z późn. zm.),
- oraz Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych - Powiatowym Urząd Pracy w Gryfinie (Zarządzenie Nr 17/20011r. Dyrektora Powiatowego Urzędu Pracy w Gryfinie z dnia 16 czerwca 20011r.) zarządzam, co następuje:

§1. Powołuję: na **Administratora Bezpieczeństwa Informacji (ABI)** w osobie:
- Pani/a ...

i **Administratora Systemów Informatycznych (ASI)** w osobie:
- Pani/a ... .

§2. Administrator bezpieczeństwa informacji i systemów informatycznych, jego zastępca odpowiedzialni są za bezpieczeństwo danych osobowych i zbioru danych rachunkowych w systemie informatycznym powiatowego urzędu pracy w Gryfinie i jego filii w Chojnie. Administratorzy obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych i rachunkowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną. Zabezpieczają dane przed ich udostępnieniem osobom nieupoważnionym, utratą, zmianą, uszkodzeniem lub zniszczeniem.

§3. Administratorzy bezpieczeństwa informacji działają zgodnie z:
- przepisami prawa w zakresie ochrony danych osobowych i ochrony zbioru danych rachunkowych,
- Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych i zbiorów danych rachunkowości w Powiatowym Urzędzie Pracy w Gryfinie i jego Filii w Chojnie.

§4. Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji - Administratorowi Systemów Informatycznych i jego zastępcy.

§5. Nadzór nad wykonaniem zarządzenia sprawują:

1. PUP Gryfino – Dyrektor i Gł. Księgowy.
2. Filia w Chojnie – z-ca Dyrektora i Księgowy Filii.

§6. Traci moc Zarządzenie Nr ... Dyrektora PUP w Gryfinie z dnia .... w sprawie powołania administratora bezpieczeństwa informacji w Powiatowym Urzędzie Pracy w Gryfinie i jego Filii w Chojnie.

§7. Zarządzenie wchodzi w życie z dniem podpisania.

Gryfino, dnia ...r.

Otrzymują:

Otrzymują:
1. Z-ca Dyrektora – Kierownik Filii w Chojnie
2. Główmy księgowy
3. Kierownicy komórek organizacyjnych
4. A/a

Zatwierdził

Załącznik nr 2

Zarządzenie dyrektora nr ..... z dnia .....

dotyczące powołania Zastępcy Administratora Bezpieczeństwa Informacji i/lub Administratora Systemów Informatycznych

Mając na uwadze ochronę danych osobowych przetwarzanych i przechowywanych w naszym systemie informatycznym od dnia ..../..../..... do dnia ..../..../..... zastępstwo Administratora Bezpieczeństwa Informacji (zwany dalej w skrócie ABI) pełni Pan/i ..... Do głównych obowiązków należą:

1. Wszelkie zadania za które odpowiedzialny jest Administrator Bezpieczeństwa Informacji.
2. Osoba zastępująca ABI składa pisemną relację z podejmowanych działań w czasie jego zastępstwa.

Szczegółowy zakres obowiązków, zadań i uprawnień ABI opisany jest/będzie w Polityce Bezpieczeństwa, przygotowywanej przez urząd

.....

Dyrektor PUP

Załącznik nr 3

PUP Gryfino

ul. Łużycka 55

74-100 Gryfino

Data

Upoważnienie nr.....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101 poz. 926 z późn. zm.)

Upoważniam

Panią/Pana .....

Zatrudnioną/ego / Odbywającą/ego staż na stanowisku

.....

.....

Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych w PUP Gryfino Upoważnienie wydaje się na czas określony do dnia ...../nieokreślony.

Zadania i czynności do wykonywania

1. Ochrona danych osobowych w systemie informatycznym i ręcznym, a w szczególności przeciwdziałanie dostępowi osób niepowołanych oraz przeciwdziałanie w przypadku wykrycia naruszeń zabezpieczeń systemu zgodnie z ustawa o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.).
2. Przestrzeganie zasad określonych w instrukcji określającej sposób zarządzania systemem informatycznym i ręcznym.
3. Przestrzeganie zasad określonych w instrukcji postępowania w sytuacji naruszania ochrony danych osobowych.
4. Przestrzeganie zachowania w tajemnicy danych osobowych uzyskanych w okresie zatrudnienie w związku z upoważnieniem do przetwarzania danych osobowych, także po ustaniu stosunku pracy.

Administrator Danych

.....

Załącznik nr 4

PUP Gryfino
ul. Łużycka 55
74-100 Gryfino
Data

Upoważnienie nr.....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101 poz. 926 z późn. zm.) oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych .

Upoważniam
Panią/Pana .....
Zatrudnioną/ego / Odbywającą/ego na stanowisku.....
do przebywania w pomieszczeniach, w których przetwarzane są dane osobowe.
Upoważnienie wydaje się na czas:
określony do dnia ...../nieokreślony.

Administrator Danych

.....

Załącznik nr 5

.....

(imię i nazwisko)

.....

(dział)

.....

(stanowisko)

OŚWIADCZENIE

Oświadczam, że zapoznałem(łam) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą z 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) oraz rozporządzeniem ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych (Dz. U Nr 100, poz. 1024) i zobowiązuję się do ich przestrzegania.

Oświadczam ponadto, że zapoznałem(łam) się z wewnętrzną instrukcją określającą sposób zarządzania systemem informatycznym, służącym przetwarzaniu danych osobowych ze szczególnym uwzględnieniem bezpieczeństwa informacji i instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

Świadomy(a) odpowiedzialności porządkowej i karnej oświadczam, że znane mi dane osobowe będę przetwarzać zgodnie z prawem, i nie dopuszczę do bezprawnego naruszenia tajemnicy również w sytuacji, gdy ustanie moje zatrudnienie w placówce:

Powiatowy Urząd Pracy w Gryfinie i filii w Chojnie:

.....

(podpis pracownika/stażysty)

Gryfino, dnia .....r.

Załącznik nr 6

Wykaz budynków, pomieszczeń lub części pomieszczeń , w których przetwarzane są dane

1. Informacje podstawowe

a) Stały dostęp do pomieszczeń przetwarzania danych osobowych mają tylko i wyłącznie upoważnieni pracownicy oraz Administrator Bezpieczeństwa Informacji i Administrator Systemu Informatycznego;

b) W pomieszczeniu przetwarzania danych po za osobami wymienionymi w punkcie 1, nie mogą przebywać inne osoby bez obecności co najmniej jednego pracownika lub bez zgody Administratora Danych.;

c) Przebywanie pracownika w pomieszczeniach przetwarzania danych po godzinach może odbyć się tylko i wyłącznie za zgodą Administratora Danych lub Administratora Bezpieczeństwa Informacji lub Administratora Systemów Informatycznych.

d) W celu ograniczenia i zabezpieczenia dostępu do pomieszczeń przetwarzania danych osobowych należy:
   - wszystkie drzwi do pomieszczeń przetwarzania danych osobowych w czasie nieobecności pracowników w tych pomieszczeniach lub zakończeniu pracy muszą być zamknięte, aby otwarcie z zewnątrz mogło nastąpić tylko i wyłącznie przez osoby uprawnione;
   - wyposażyć pomieszczania, gdzie przechowywane są kartoteki w system przeciwpożarowy i przeciwwłamaniowy;
   - pomieszczenie, w którym znajdują się serwery należy wyposażyć w system klimatyzacji, przeciwpożarowy i przeciwwłamaniowy;

e) Prace techniczne wykonywane przez osoby trzecie w pomieszczeniach przetwarzania danych mogą odbywać się jedynie w obecności co najmniej jednego pracownika lub za zgodą Administratora Danych oraz po uprzednim poinformowaniu kierownika

jednostki. W trakcie wykonywania prac technicznych przez osoby trzecie w pomieszczeniu przetwarzania danych, w którym trwają prace przetwarzanie danych jest zabronione.

2. Wykaz pomieszczeń w których przetwarzane są dane osobowe.

1. Powiatowy Urząd Pracy w Gryfinie – ul. Łużycka 55, 74-100 Gryfino
    a. Centrum Aktywizacji Zawodowej – pomieszczenia nr 4,7,9,10
    b. Referat ds. ewidencji i świadczeń – pomieszczenia nr 5,6
    c. Referat ds. organizacyjno-administracyjny – pomieszczenia nr 1,2,3, archiwum, pomieszczenie informatyka, serwerownia
    d. Referat ds. finansowo-księgowych – pomieszczenia nr 8,11
2. Powiatowy Urząd Pracy w Gryfinie Filia w Chojnie – ul. Dworcowa 3, 74-500 Chojna
    a. Centrum Aktywizacji Zawodowej – pomieszczenia nr 10,11,12,21,22,32
    b. Referat ds. ewidencji i świadczeń – pomieszczenia nr 17,31
    c. Referat ds. organizacyjno-administracyjny – pomieszczenia nr 18,19,20,33
    d. Referat ds. finansowo-księgowych – pomieszczenia nr 23,30

Załącznik nr 7

Wykaz zbiorów przetwarzanych elektronicznie lub w inny sposób

1. W celu ochrony przed utratą danych w PUP Gryfino stosowane są następujące zabezpieczenia:
   a) ochrona serwerów przed zanikiem i wahaniami zasilania poprzez stosowanie zasilaczy zapasowych UPS,
   b) ochrona newralgicznych elementów sieciowych przed zanikiem zasilania,
   c) ochrona przed utratą zgromadzonych danych przez robienie codziennych kopii zapasowych, z których w przypadku awarii odtwarzane są dane,

2. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych:
   d) podłączenia danego użytkownika do szkieletu sieci komputerowej dokonuje Administrator Bezpieczeństwa Informacji,
   e) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa Informacji z wnioskiem w którym podane będą dane nowego użytkownika oraz zasoby jakie mają być udostępnione,
   f) w systemie informatycznym PUP Gryfino zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do stacji podając login oraz hasło. Drugiej autoryzacji należy dokonać uruchamiając program użytkowy służący do przetwarzania danych osobowych, podając inny login użytkownika oraz hasło. Dostęp do wybranej bazy danych uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego.

3. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych PUP Gryfino poprzez Internet. W zakresie dostępu do sieci wewnętrznej Urzędu z rozległej sieci Internet zastosowano środki ochrony przed dostępem z zewnątrz. W PUP Gryfino zastosowano system wykrywający obecność wirusów w poczcie elektronicznej.

W efekcie zapewnione jest:

- zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wszystkich zbędnych portów,
- objęcie ochroną antywirusową wszystkich danych ściąganych z sieci Internet na stacjach lokalnych.

4. Postanowienia końcowe.
   g) zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Bezpieczeństwa Informacji zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,
   h) osoby mające dostęp do danych muszą posiadać zaświadczenie o przebytym szkoleniu z zakresu ustawy o ochronie danych osobowych z dnia 29.08.1997r.,
   i) w pomieszczeniu z serwerami musi znajdować się gaśnica, która jest okresowo napełniana i kontrolowana przez specjalistę.

Wykaz zbiorów.

Lp.	Nazwa zbioru	Program zastosowany do przetwarzania	Pomieszczenie, w którym przetwarza się dane	Nazwa urządzenia, w którym znajdują się dane osobowe
1.	Ewidencja bezrobotnych i klientów Powiatowego Urzędu Pracy w Gryfinie	• Syriusz • PULS • Płatnik • SEPI • Forma tradycyjna	Gryfino pokoje nr: 1,2,3,4,5,6,7,8,9,10,serwerownia , archiwum, pomieszczenie informatyka; Chojna pokoje nr: 1,2,3,4,5,6,7,10.11.1217,18,19,20,21,22,23,30,31,32,33	Serwery, stacje robocze
2.	Kancelaria BIP	• Kancelaria BIP	Gryfino pokoje nr: 1,2,3,4,5,6,7,8,9,10,serwerownia , archiwum, pomieszczenie informatyka; Chojna pokoje nr: 1,2,3,4,5,6,7,10.11.1217,18,19,20,21,22,23,30,31,32,33	Serwery, stacje robocze
3.	Dokumentacja pracowników Urzędu	• Syriusz • PULS • Płatnik • Forma tradycyjna	Gryfino pokoje nr: 1, archiwum	Serwery, stacje robocze
4.	Podsystem Monitoringu Europejskiego Funduszu Społecznego	• PEFS2007	Gryfino pokoje nr: 9 Chojna pokój nr: 32	Serwery, stacje robocze
5.	Aplikacje kandydatów do pracy CV	• Kancelaria BIP • Forma tradycyjna • Outlook	Gryfino pokoje nr: 1,2,3, archiwum Chojna pokoje nr: 19	Serwery, stacje robocze
6.	Umowy cywilno-prawne z osobami fizycznymi	• Forma tradycyjna	Gryfino pokoje nr: 1,2,3,4,5,6,7,8,9,10,serwerownia , archiwum, pomieszczenie informatyka; Chojna pokoje nr: 1,2,3,4,5,6,7,10.11.1217,18,19,20,21,22,23,30,31,32,33,	

Załącznik nr 8

PUP Gryfino
ul. Łużycka 55
74-100 Gryfino
Data

Wniosek o przeszkolenie przez Administratora Bezpieczeństwa Informacji

Zwracam się z uprzejmą prośbą o przeszkolenie z Polityk Bezpieczeństwa p. ..... zatrudnioną/ego / odbywającą/ego staż od dnia..... do dnia..... na stanowisku ..... w Referacie.....

.....
Pracownik ds. kadr

Załącznik nr 9

PUP Gryfino
ul. Łużycka 55
74-100 Gryfino
Data

Osoba wnioskująca
Imię i nazwisko.....
stanowisko .....

WNIOSEK O ZAREJESTROWANIE/WYREJESTROWANIE UŻYTKOWNIKA

Na podstawie Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
Proszę o zarejestrowanie/wyrejestrowanie w systemie informatycznym użytkownika dla:
Pani/Pana.....
Stanowisko .....
Referat.....
Parametry dostępu:

Program	Dostęp
Syriusz	tak/nie
Puls	tak/nie
Płatnik	tak/nie
SEPI	tak/nie
Novell	tak/nie
Home Banking	tak/nie
Ekonto	tak/nie

.....

.....
Podpis Przełożonego

Wyrażam zgodę/Nie wyrażam zgody

.....
Podpis ABI

Załącznik nr 10

Ewidencji osób upoważnionych do przetwarzania danych osobowych

lp	Imię i nazwisko	Identyfikator	Data nadania upoważnienia	Data zakończenia upoważnienia	Nr upoważnienia	Zakres upoważnienia

Załącznik nr 11

Wzór raportu z naruszenia zasad bezpieczeństwa systemu informatycznego w PUP Gryfino

1. Data:..... Godzina:.....

2. Osoba powiadamiająca o zaistniałym zdarzeniu: .....

   .....
   (Imię i Nazwisko, stanowisko służbowe)

3. Lokalizacja zdarzenia: .....
   (np. nr pokoju; nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa, oraz okoliczności towarzyszące:

   .....

   .....

   .....

5. Podjęte działania:

   .....

   .....

6. Przyczyny wystąpienia zdarzenia:

   .....

   .....

7. Postępowanie wyjaśniające:

   .....

   .....

.....
data, podpis

Załącznik nr 12

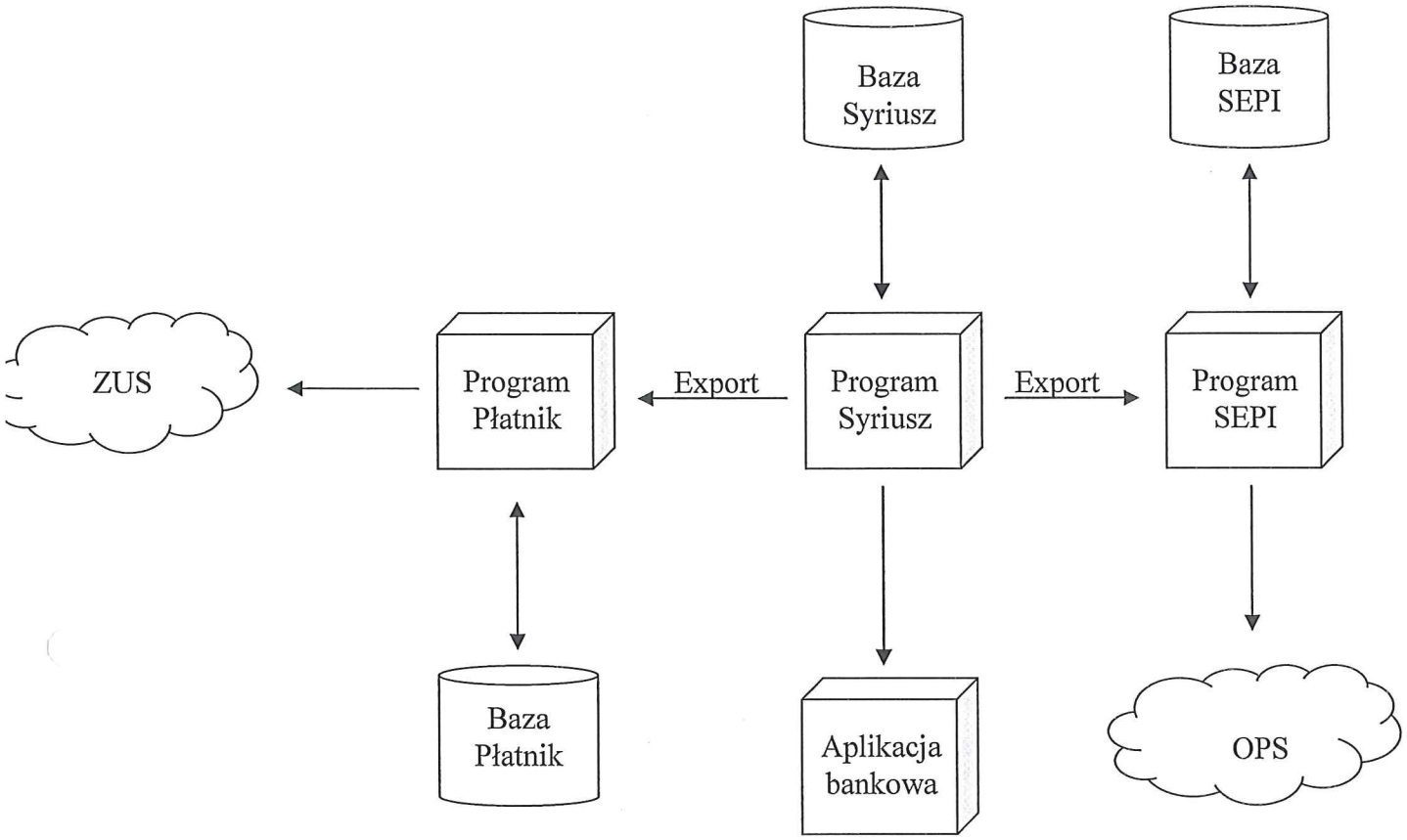
Opis struktur zbiorów danych wskazujący zawartości poszczególnych pól informacyjnych i powiązania między nimi.

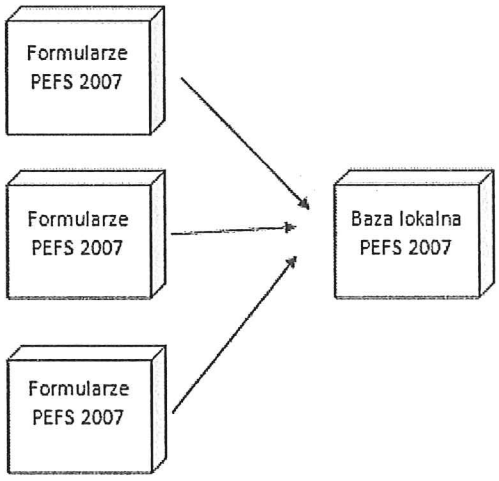
1. Podstawowe zbiory danych przetwarzanych w Powiatowym Urzędzie Pracy w Gryfinie przetwarzane są w programach:
   1) Word – Writer
   2) Excel – Calc
   3) Syriusz
   4) PULS
   5) Płatnik
   6) PEFS 2007
   7) SEPI
2. Struktura bazy danych programu Syriusz Std dołączona została do dokumentu, jako kolejny załącznik
3. Struktura bazy programu Płatnik została dodana do niniejszego dokumentu, jako kolejny załącznik.
4. Bazy danych programu PULS jest już tylko bazą archiwalną, nie są wprowadzane do niej nowe elementy. Obecnie baza programu PULS służy tylko, jako baza archiwalna Struktura bazy danych programu została dołączona do dokumentu, jako kolejny załącznik.
5. Struktura bazy aplikacji Podsystemu Monitoringu Europejskiego Funduszu Społecznego – PEFS 2007 została dołączona do dokumentacji, jako kolejny załącznik.
6. W aplikacja biurowych takich jak: WORD, Write, Excel, Calc tworzone są zbiory bez określonych i trwałych struktur.

Załącznik nr

Sposób przepływu danych pomiędzy poszczególnymi systemami.

1. Baza programu jak i sama aplikacja dostępu do bazy PULS jest już tylko bazą archiwalną. Została dokonana migracja danych z bazy programu PULS do bazy programu Syriusz.
2. Dane w systemie Syriusz wprowadzane są przez pracowników do bazy na poszczególnych jednostkach komputerowych. Wszystkie informacje przesyłane są do serwera i tam też są przechowywane. Odczyt danych lub ich wszelka modyfikacja wykonywana jest na stanowiskach pracowników posiadających swoje konta w systemie. Przepływ danych ma także miejsce w momencie przesyłania plików z Syriusza do programu Płatnik. Podczas takiego działania w Syriuszu generowany jest plik zawierający informacje o operacjach finansowych. Plik ten z kolei odczytywany jest w programie Płatnik, w którym dokonywane są dalsze czynności.
3. Dane w aplikacji PEFS 2007 są wpisywane przez pracowników korzystających z aplikacji. Następnie dane z pojedynczych plików aplikacji importowane są do całkowitej bazy PEFS2007 przez pracownika Urzędu.
4. Dokładny przepływ danych pomiędzy systemami informatycznymi obrazują zamieszczone poniżej grafiki.


Baza
Syriusz
Baza
SEPI
ZUS
Program
Płatnik
Export
Program
Syriusz
Export
Program
SEPI
Baza
Płatnik
Aplikacja
bankowa
OPS


Formularze
PEFS 2007
Formularze
PEFS 2007
Formularze
PEFS 2007
Baza lokalna
PEFS 2007